PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

□ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	09/777,032
Filing Date	February 5, 2001
First Named Inventor	Stephen A. BAGSHAW
Examiner Name	Matthew HENEGHAN
Art Unit	2134
Attorney Docket No.	1376-0100030

METHOD OF PAYMENT (check all that apply)

□ Check □ Credit Card □ Money Order □ None □ Other (please identify): ____________

☑ Deposit Account Deposit Account Number: 50-0441 Deposit Account Name: ATI Technologies, Inc.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below □ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims Extra Claims Fee ($) Fee Paid ($)
________ - 20 or HP = ________ x ________ = ________
HP = highest number of total claims paid for, if greater than 20.

Multiple Dependent Claims
Fee ($) ________ Fee Paid ($) ________

Indep. Claims Extra Claims Fee ($) Fee Paid ($)
________ - 3 or HP = ________ x ________ = ________
HP = highest number of independent claims paid for, if greater than 3.

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets Extra Sheets Number of each additional 50 or fraction thereof Fee ($) Fee Paid ($)
________ - 100 = ________ / 50 = ________ (round up to a whole number) x ________ = ________

4. OTHER FEE(S) Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) ________

Other (e.g., late filing surcharge): Appeal Brief 500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 51,596	Telephone 512-439-7100
Name (Print/Type)	Ryan S. Davidson		Date 3/9/06

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Stephen A. BAGSHAW

FOR: METHOD AND SYSTEM FOR DUAL LINK COMMUNICATIONS ENCRYPTION

App. No.:	09/777,032	App. No.:	09/777,032
Examiner:	HENEGHAN, Matthew	Customer No.:	34456
Atty. Dkt. No.:	1376-0100030	Atty. Dkt. No.:	1376-0100030

Mail Stop APPEAL BRIEF-PATENTS
The Board of Patent Appeal and Interferences
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Ryan S. Davidson, Reg. No. 51,596
LARSON NEWMAN ABEL POLANSKY & WHITE, LLP
(512) 439-7100 (phone)
(512) 327-5452 (fax)

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(1)):

TABLE OF CONTENTS

The final page of this brief before the beginning of the Appendix of Claims bears the agent's signature.

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is ATI Technologies, Inc.

II. RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c)(1)(ii))

There are no interferences or other appeals that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS (37 C.F.R. § 41.37(c)(1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

There are thirty-one (31) claims pending in the application (claims 1-5, 7-13, 15-17, 19-27, and 29-35).

B. STATUS OF ALL THE CLAIMS

1. Claims pending:

   Claims 1-5, 7-13, 15-17, 19-27, and 29-35

2. Claims withdrawn from consideration but not canceled:

   NONE.

3. Claims allowed:

   NONE.

4. Claims objected to:

   Claims 7, 8, 10, 13, 15, 19, 29, 30, and 32-34.

5. Claims rejected:

   Claims 1, 2, 4, 9, 11, 12, 16, 20, 25, 26, and 31 are rejected under 35 U.S.C. § 102(e).

   Claims 3, 5, 17, 21-24, 27, and 32 are rejected under 35 U.S.C. § 103(a).

6. Claims canceled:

Claims 6, 14, 18, and 28.

C. CLAIMS ON APPEAL

There are four (4) claims on appeal, claims 1, 12, 25, and 26.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

Amendments to claims 4 and 25 were submitted subsequent to the Final Office Action dated June 15, 2005. The Advisory Action mailed August 23, 2005 does not indicate whether these amendments were entered. These amendments were directed to correcting informalities (i.e., the addition of the term "and" before the last claim element and the replacement of an errant semicolon with a period) and do not affect the scope of the claims. Accordingly, it is assumed that these amendments were entered.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

The following summary is provided to give the Board the ability to quickly determine where the claimed subject matter appealed herein is described in the Present Application and is not to limit the scope of the claimed invention.

Independent claim 1 recites the features of receiving a single digital data stream. Claim 1 further recites the features of encrypting a first portion of the single digital data stream with a first encryption key to generate a first encrypted stream and encrypting a second portion of the single digital data stream with a second encryption key to generate a second encrypted stream.

Independent claim 12 recites the features of a data processor having a first I/O buffer and a memory having a second I/O buffer coupled to the first I/O buffer of the data processor. The memory is capable of storing code for establishing a set of encrypted links between a peripheral device and a software component. Establishing a first encrypted link of the set of encrypted links includes generating a first encryption key associated with a first port of encrypted data and establishing a second encrypted link of the set of encrypted links includes generating a second encryption key associated with a second port of encrypted data. Claim 12 further recites the features of a hardware controller capable of outputting the first and the second encrypted links. The hardware controller includes a first register capable of storing information associated with the first encryption key, a second register capable of storing information associated with the second encryption key, and a cipher component. The cipher component is capable of receiving a single digital data stream, applying the first encryption key to a first portion of the data stream, and applying the second encryption key to a second portion of the data stream. The hardware controller further includes a de-multiplexing component capable of splitting the single data stream into multiple data streams.

Independent claim 25 recites the feature of an interface capable of receiving a first and a second link of encrypted data from a hardware controller. Claim 25 further recites the feature of a first decryption component capable of decrypting the first link of encrypted data, using a first encryption key, to generate a first portion of a single received digital data stream and a second decryption component capable of decrypting the second link of encrypted data, using a second encryption key, to generate a second portion of the received digital data stream. Claim 25 further recites the feature of a multiplexing component capable of combining the first and the second portions of the received data streams to form a single received digital data stream.

FIG. 5 and the corresponding passage of the Present Application at page 15, line 9 – page 20, line 25 illustrate a particular implementation of the claimed subject matter of claims 1, 12 and 25. As taught by the Present Application, a single data stream 516 (i.e., the claimed "single digital data stream") is received at the video controller 510 (i.e., the claimed "hardware controller"). In this example, the single data stream 516 contains interweaved even pixel data set A (i.e., the claimed "first portion of the single digital data stream") and odd pixel data set B (i.e., the claimed "second portion of the single digital data stream"). The LFSR module 532 generates pseudo random numbers for use in generating encryption keys for the single data stream 516, where an even key (i.e., the claimed "first encryption key") is generated for the even pixel data set A and an odd key (i.e., the claimed "second encryption key") is generated for the odd pixel data set B of the single data stream 516. The even key is stored in the even register 512 (i.e., the claimed "first register") and the odd key is stored in the odd register 511 (i.e., the claimed "second register"). The output function 536 (i.e., the claimed "cipher component") encrypts the single data stream 516, using the even encryption key to encrypt the even pixel data set A and the odd encryption key to encrypt the odd pixel data set B. The resulting encrypted data stream

539 is demultiplexed by the de-multiplexing component 540 (i.e., the claimed "de-multiplexing component") to provide an even pixel data stream C (i.e., the claimed "first encrypted stream") containing encrypted even pixel data and to provide an odd pixel data stream D (i.e., the claimed "second encrypted stream")(together, the claimed "multiple data streams").

The even pixel data stream C and the odd pixel data stream D then are provided to a transmission-minimized differential signaling (TMDS) receiver 552 (i.e., the claimed "interface") from the video controller 510 via the digital video output (DVO) port 546 and the TMDS transmitter 550, where the TMDS transmitter 550 and the TMDS receiver 552 can utilize two separate links (i.e., the claimed "first and second link of encrypted data"), one for the even pixel data stream C and one for the odd pixel data stream D. The TMDS receiver 552 uses the first HDCP component 562 (i.e., the claimed "first decryption component") to decrypt the even pixel data stream C and the second HDCP component 564 (i.e., the claimed "second decryption component") to decrypt the odd pixel data stream D. The multiplexing component 570 (i.e., the claimed "multiplexing component") merges the data provided from the first HDCP component 562 with the data provided from the second HDCP component 564 to generate a merged data stream (i.e., the claimed "single received digital data stream").

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1, 12, 25, and 26 are rejected under 35 U.S.C. § 102(e) in view of United States Patent No. 6,157,719 to Wasilewski et al. (hereinafter, "the Wasilewski reference") as set forth in the Final Office Action dated June 15, 2005 (hereinafter, "the Final Action") and the Advisory Action dated August 23, 2005 (hereinafter, "the Advisory Action").

VII. ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

Based on the arguments and issues below, none of the claims stand or fall together, because in addition to having different scopes, each of the independent claims has a unique set of issues relating to its rejection and appeal as indicated in the arguments below.

A. Rejection of Claim 1 under 35 U.S.C. § 102(e):

At page 4 of the Final Action, claim 1 was rejected under 35 U.S.C. § 102(e) as being anticipated by the Wasilewski reference. The Final Action asserts that the Wasilewski reference discloses all of the features recited by claim 1 and the Advisory Action reaffirms this position. Contrary to the assertions of the Final Action and the Advisory Action, the Wasilewski reference fails to disclose each and every feature recited by claim 1 for at least the reasons provided below.

Under 35 U.S.C. § 102, the Patent Office bears the burden of presenting at least a prima facie case of anticipation. In re Sun, 31 USPQ2d 1451, 1453 (Fed. Cir. 1993) (unpublished). Anticipation requires that a prior art reference disclose, either expressly or under the principles of inherency, each and every element of the claimed invention. Id. "In addition, the prior art reference must be enabling." Akzo N.V. v. U.S. International Trade Commission, 808 F.2d 1471, 1479, 1 USPQ2d 1241, 1245 (Fed. Cir. 1986), cert. denied, 482 U.S. 909 (1987). That is, the prior art reference must sufficiently describe the claimed invention so as to have placed the public in possession of it. In re Donohue, 766 F.2d 531, 533, 226 USPQ 619, 621 (Fed. Cir. 1985). "Such possession is effected if one of ordinary skill in the art could have combined the publication's description of the invention with his own knowledge to make the claimed invention." Id.

Independent claim 1 is reproduced below for ease of reference:

1. (Previously Presented) A method comprising:
receiving a single digital data stream;
encrypting a first portion of the single digital data stream with a first encryption key to generate a first encrypted stream; and
encrypting a second portion of the single digital data stream with a second encryption key to generate a second encrypted stream.

a) *The Wasilewski reference fails to disclose receiving a single digital data stream and encrypting first and second portions of the received single data stream using first and second encryption keys, respectively, to generate first and second encrypted streams, respectively, as recited by claim 1*

Claim 1 recites the features of receiving a *single* digital data stream, encrypting *a first portion of the single digital data stream* with a first encryption key to *generate a first encrypted* *stream* and encrypting *a second portion of the single digital data stream* with a second encryption key to *generate a second encrypted stream.* At paragraph 6, the Final Action asserts that the passage of the Wasilewski reference at column 6, lines 24-27 and FIG. 2A disclose the specific combination of features of claim 1. For ease of reference, a portion of the Wasilewski reference including the relied-upon passage is reproduced below:

> In FIG. 2A, clear services such as the elementary digital bit streams which comprise MPEG-2 programs are sent through a 1st level encryption called the Program Encrypt function 201, which is preferably a symmetric cipher such as the well-known DES algorithm. Each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be combined with other elementary streams and private data, such as conditional access data.

The Wasilewski Reference, Column 6, Lines 24-33 (emphasis added).

In view of this cited passage, the Final Action asserts that claim 1 is anticipated for the reason that in "the digital cable (video) television system disclosed by [the Wasilewski reference], a set of any number of bit streams (such as 2 streams) are combined and each of several bit streams are individually encrypted at a the Program Encrypt function 201." Final Action, p. 4. However, this assertion is contrary to the recited features of claim 1. As the cited passage illustrates, the Wasilewski reference discloses that "each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be combined with other elementary streams." Id. The Wasilewski reference therefore teaches that multiple streams may be individually encrypted and then combined or merged by the MUX 200 to generate a single stream (i.e., the output of the MUX 200). In sharp contrast, claim 1 provides that a single digital data stream is received and a first encrypted stream and a second encrypted stream are generated from the single digital data stream. Thus, the Wasilewski reference teaches the *merging* of multiple separate encrypted streams to generate a single stream, whereas the subject matter of claim 1 is directed to the *separation* of a single data stream into multiple encrypted streams. Accordingly, contrary to the assertions of Final Action and the Advisory Action, neither the relied-upon passage of the Wasilewski reference nor any other passage of the Wasilewski reference discloses receiving a single digital data stream and encrypting first and second portions of the received single data stream using first and second encryption keys, respectively, to generate first and second encrypted streams, respectively, as provided by claim 1.

b) *The Wasilewski reference fails to anticipate claim 1*

As established above, the Wasilewski reference fails to disclose at least one feature recited by claim 1 and therefore fails to disclose each and every feature of claim 1. Claim 1 therefore is allowable under 35 U.S.C. § 102(e).

B. Rejection of Claim 12 under 35 U.S.C. § 102(e):

At page 4 of the Final Action, claim 12 is rejected under 35 U.S.C. § 102(e) as anticipated by the Wasilewski reference. The Final Action asserts that the Wasilewski reference discloses all of the features recited by claim 12 and the Advisory Action reaffirms this position. Contrary to the assertions of the Final Action and the Advisory Action, the Wasilewski reference fails to disclose each and every feature recited by claim 12 for at least the reasons provided below.

Independent claim 12 is reproduced below for ease of reference:

> 12. (Previously Presented) A system comprising:
> a data processor having a first I/O buffer;
> a memory having a second I/O buffer coupled to the first I/O buffer of the data processor, the memory capable of storing code for:
> establishing a set of encrypted links between a peripheral device and a software component; wherein establishing a first encrypted link of the set of encrypted links includes generating a first encryption key associated with a first port of encrypted data and establishing a second encrypted link of the set of encrypted links includes generating a second encryption key associated with a second port of encrypted data;
> a hardware controller capable of outputting the first and the second encrypted links, wherein the hardware controller includes:
> a first register capable of storing information associated with the first encryption key;
> a second register capable of storing information associated with the second encryption key;
> a cipher component capable of :
> receiving a single digital data stream;
> applying the first encryption key to a first portion of the data stream; and
> applying the second encryption key to a second portion of the data stream; and

a de-multiplexing component capable of splitting the single data stream into multiple data streams.

a) *The Wasilewski reference fails to disclose a cipher component as recited by claim 12*

Claim 12 recites the features of a cipher component capable of receiving a single digital data stream, applying the first encryption key to a first portion of the data stream, and applying the second encryption key to a second portion of the data stream. With respect to claim 12, the Final Action merely provides "[a]s per claim 12, 16, 20, 25 and 31, the invention is implemented using set-top boxes, which inherently have I/O buffers for data transfers, and registers to hold the keys being used. Two decryptors are used to create the combined data stream in FIG. 2B." Final Action, p. 4. It is noted that this statement does not address the identified feature of claim 12 in any manner. Regardless, as discussed above with respect to claim 1, the Wasilewski reference teaches only that elementary streams may be "individually encrypted," but fails to disclose that a first encryption key is applied to a first portion of an elementary stream and a second encryption key is applied to a second portion of the elementary stream as would be consistent with claim 12. Thus, the Wasilewski reference fails to disclose the cipher component feature as recited by claim 12.

b) *The Wasilewski reference fails to disclose a de-multiplexing component as recited by claim 12*

Claim 12 further recites the feature of a de-multiplexing component capable of splitting the single data stream into multiple data streams. As noted above, the Final Action fails to specifically address the manner in which the Wasilewski reference discloses this feature. See Final Action, p. 4. Regardless, the passage of the Wasilewski reference cited by the Final Action in reference to claim 1 provides that multiple encrypted elementary data streams can be combined by a MUX 200, whereas claim 12 recites a de-multiplexing component capable of splitting the single data stream into multiple data streams. Thus, the Wasilewski reference fails to disclose the de-multiplexing component as recited by claim 12.

c) *The Wasilewski reference fails to anticipate claim 12*

As established above, the Wasilewski reference fails to disclose at least one of the features recited by claim 12 and therefore fails to disclose each and every feature recited by claim 12. Claim 12 therefore is allowable under 35 U.S.C § 102(e).

C. Rejection of Claim 25 under 35 U.S.C. § 102(e):

At page 4 of the Final Action, claim 25 is rejected under 35 U.S.C. § 102(e) as anticipated by the Wasilewski reference. The Final Action asserts that the Wasilewski reference discloses all of the features recited by claim 25 and the Advisory Action reaffirms this position. Contrary to the assertions of the Final Action and the Advisory Action, the Wasilewski reference fails to disclose each and every feature recited by claim 25 for at least the reasons provided below.

Independent claim 25 is reproduced below for ease of reference:

25. (Previously Presented) A system comprising:
an interface capable of receiving a first and a second link of encrypted data from a hardware controller;
a first decryption component capable of decrypting the first link of encrypted data, using a first encryption key, to generate a first portion of a single received digital data stream;
a second decryption component capable of decrypting the second link of encrypted data using a second encryption key to generate a second portion of the received digital data stream; and
a multiplexing component capable of combining the first and the second portions of the received data streams to form a single received digital data stream.

a) *The Wasilewski reference fails to disclose an interface capable of receiving a first and a second link of encrypted data from a hardware controller as recited by claim 25*

Claim 25 recites the features of an interface capable of receiving a first and a second link of encrypted data from a hardware controller. With respect to claim 25, the Final Action merely provides that "[a]s per claim 12, 16, 20, 25 and 31, the invention is implemented using set-top boxes, which inherently have I/O buffers for data transfers, and registers to hold the keys being used. Two decryptors are used to create the combined data stream in FIG. 2B." Final Action, p. 4. It is noted that this statement does not address the claimed interface feature of claim 25 in any manner. Regardless, the Wasilewski reference fails to disclose an interface capable of receiving a first and a second link of encrypted data as provided by claim 25. To illustrate, the demultiplexer 230 of FIG. 2B of the Wasilewski reference receives only a single transport data stream (i.e., only a single link of encrypted data). See the Wasilewski Reference, Column 7, Lines 6 – 24. Further, the Wasilewski reference fails to disclose that any of the components that receive, provide or otherwise process encrypted data is a hardware controller, whereas claim 25 provides that the interface is capable of receiving a first and a second link of encrypted data from a hardware controller. Thus, the Wasilewski reference fails to disclose the interface feature as recited by claim 25.

b) *The Wasilewski reference fails to disclose a first decryption component and a second decryption component capable of decrypting the first link of encrypted data and second link of encrypted data, respectively, to generate a first portion and a second portion, respectively, of a single received digital data stream as recited by claim 25*

Claim 25 further recites the features of a first decryption component capable of decrypting the first link of encrypted data, using a first encryption key, to generate a first portion of a single received digital data stream, and a second decryption component capable of decrypting the second link of encrypted data using a second encryption key to generate a second portion of the received digital data stream. With respect to these features, the Final Action merely states that "[t]wo decryptors are used to create the combined data stream in FIG. 2B." See Final Action, p. 4. In contrast with the assertions of the Final Action, the Wasilewski reference fails to disclose that "two decryptors are used to create the combined data stream." Rather, the Wasilewski reference teaches that a transport data stream is received at the demultiplexer 230, where an encrypted multisession key ($E_{K_{pr}}$(MSK)) is decrypted by the decryptor 234 and the decrypted multisession key is used by the decryptor 236 to decrypt an encrypted codeword (E_{MSK}(CW)). The Wasilewski Reference, Column 7, Lines 8-20 and FIG. 2B. The Wasilewski reference further teaches that the decrypted codeword is used by the decryptor 238 to decrypt an encrypted service (E_{CW}(SERVICE)). Id. Thus, rather than teaching first and second decryption components capable of decrypting respective links of encrypted data to generate respective portions of a single received digital data stream as would be consistent with claim 25, the Wasilewski reference teaches the decryption of a mask value, which is used to decrypt a codeword, which is then used to decrypt a single service. Thus, the Wasilewski reference fails to disclose the first and second decryption components as recited by claim 25.

c) *The Wasilewski reference fails to anticipate claim 25*

As established above, the Wasilewski reference fails to disclose at least one of the features recited by claim 25 and therefore fails to disclose each and every feature recited by claim 25. Claim 25 therefore is allowable under 35 U.S.C § 102(e).

D. Rejection of Claim 26 under 35 U.S.C. § 102(e)

At page 4 of the Final Action, claim 26 is rejected under 35 U.S.C. § 102(e) as anticipated by the Wasilewski reference. The Final Action asserts that the Wasilewski reference discloses all of the features recited by claim 25 and the Advisory Action reaffirms this position. Contrary to the assertions of the Final Action and the Advisory Action, the Wasilewski reference fails to disclose each and every feature recited by claim 25 for at least the reasons provided below.

Claim 26, which depends from claim 25, is reproduced below for ease of reference: -

> 26. (Original) The system as in Claim 25, further including:
> a clock capable of clocking the single received data stream at twice the speed of the first and second links of encrypted data; and
> a single processing component capable of processing the data associated with the first and the second links of encrypted data.

a) *The clock feature recited by claim 26 is neither explicitly disclosed by, nor inherent to, the Wasilewski reference*

Claim 26 recites the feature of a clock capable of clocking the single received data stream at twice the speed of the first and second links of encrypted data. With respect to this feature, the Final Action asserted that "all modern computer systems use programmable counter/timers that are capable of clocking one stream at twice the speed of others." Final Action, p. 4. In the Response to the Final Action mailed August 5, 2004 (hereinafter, "the Final Response"), the Appellant noted that the Final Action was relying on an "Official Notice" –type argument, which is improper in an anticipation (§ 102) rejection. The Appellant therefore requested that the anticipation rejection of claim 26 be withdrawn or that the Office cite a reference in support of its assertion. Subsequently, the Advisory Action changed position with respect to claim 26 and asserted that the claimed feature of a clock capable of clocking the single received data stream at twice the speed of the first and second links of encrypted data is inherent to the disclosure of the Wasilewski reference, rather than being obvious in view of the Wasilewski reference. See Advisory Action, p. 2.

As provided by the M.P.E.P.,

> The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. In re Rijckaert, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); In re Oelrich, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted) . . .[emphasis added]. . . .
>
> "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." Ex parte Levy, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original) (Applicant's invention was directed to a biaxially oriented, flexible dilation catheter balloon (a tube which expands upon inflation) used, for example, in clearing the blood vessels of heart patients). The examiner applied a U.S. patent to Schjeldahl which disclosed injection molding a tubular preform and then injecting air into the preform to expand it against a mold (blow molding). The reference did not directly state that the end product balloon was biaxially oriented. It did disclose that the balloon was "formed from a thin flexible inelastic, high tensile strength, biaxially oriented synthetic plastic material." *Id.* at 1462 (emphasis in original). The examiner argued that Schjeldahl's balloon was inherently biaxially oriented. The Board reversed on the basis that the examiner did not provide objective evidence or cogent technical reasoning to support the conclusion of inherency.

M.P.E.P § 2112(IV).

As described by the above-cited passage of the M.P.E.P, the burden of proof for establishing that a claim feature is inherent initially rests with the Patent Office. It is noted that neither the Final Action nor the Advisory Action provide "a basis in fact and/or technical reasoning to reasonable support the determination that the allegedly inherent characteristic necessarily flows from the teachings" of the Wasilewski reference. See Id. (citing Ex parte Levy). Instead, the Advisory Action merely makes a generalized allegation that the clock feature of claim 26 is inherent to the Wasilewski reference. Accordingly, the Final Action and the Advisory Action fail to establish a *prima facie* case of inherency with respect to the clock feature recited by claim 26.

c) *The Wasilewski reference fails to anticipate claim 26*

As established above, the Wasilewski reference fails to disclose the features recited by claim 26 at least by virtue of its dependency from claim 25. Moreover, the Patent Office fails to establish that at least one feature recited by claim 26 is explicitly disclosed by or inherent to the Wasilewski reference. The Patent Office therefore fails to establish a *prima facie* case of anticipation for claim 26. Claim 26 therefore is allowable under 35 U.S.C § 102(e).

VIII. CONCLUSION

For the reasons given above, the Appellant respectfully requests reconsideration and allowance of all claims and that this patent application be passed to issue.

Respectfully submitted,

9 March 2006
Date

Ryan S. Davidson, Reg. No. 51,596
LARSON NEWMAN ABEL POLANSKY & WHITE, LLP
(512) 439-7100 (phone)
(512) 327-5452 (fax)

IX. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(viii))

The text of each claim involved in the appeal is as follows:

1. (Previously Presented) A method comprising:

receiving a single digital data stream;

encrypting a first portion of the single digital data stream with a first encryption key to generate a first encrypted stream; and

encrypting a second portion of the single digital data stream with a second encryption key to generate a second encrypted stream.

12. (Previously Presented) A system comprising:

a data processor having a first I/O buffer;

a memory having a second I/O buffer coupled to the first I/O buffer of the data processor, the memory capable of storing code for:

establishing a set of encrypted links between a peripheral device and a software component, wherein establishing a first encrypted link of the set of encrypted links includes generating a first encryption key associated with a first port of encrypted data and establishing a second encrypted link of the set of encrypted links includes generating a second encryption key associated with a second port of encrypted data;

a hardware controller capable of outputting the first and the second encrypted links, wherein the hardware controller includes:

a first register capable of storing information associated with the first encryption key;

a second register capable of storing information associated with the second encryption key;

a cipher component capable of :

receiving a single digital data stream;

applying the first encryption key to a first portion of the data stream; and applying the second encryption key to a second portion of the data stream; and

a de-multiplexing component capable of splitting the single data stream into multiple data streams.

25. (Previously Presented) A system comprising:

an interface capable of receiving a first and a second link of encrypted data from a hardware controller;

a first decryption component capable of decrypting the first link of encrypted data, using a first encryption key, to generate a first portion of a single received digital data stream;

a second decryption component capable of decrypting the second link of encrypted data using a second encryption key to generate a second portion of the received digital data stream; and

a multiplexing component capable of combining the first and the second portions of the received data streams to form a single received digital data stream.

26. (Original) The system as in Claim 25, further including:

a clock capable of clocking the single received data stream at twice the speed of the first and second links of encrypted data; and

a single processing component capable of processing the data associated with the first and the second links of encrypted data.

X. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

None.

XI. RELATED PROCEEDINGS APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

None.